UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/853,770	05/11/2001	Satoshi Shigematsu	96790P355	6640

8791 7590 12/27/2007
BLAKELY SOKOLOFF TAYLOR & ZAFMAN
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
TRAN, ELLEN C	
ART UNIT	**PAPER NUMBER**
2134	
MAIL DATE	**DELIVERY MODE**
12/27/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

60

Office Action Summary	**Application No.** 09/853,770	**Applicant(s)** SHIGEMATSU ET AL.	
	Examiner Ellen C. Tran	**Art Unit** 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 October 2007*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4-36 and 83-93* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4-36 and 83-93* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)☒ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.☒ Certified copies of the priority documents have been received in Application No. 09/853,770.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Ellen Tran
ELLEN TRAN
PATENT EXAMINER
ART 2134

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *29 Oct. 2007*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) □ Notice of Informal Patent Application
6) □ Other: _____.

DETAILED ACTION

1. This action is responsive to communication: filed on 10 October 2007 with an original application filed 11 May 2001, with acknowledgement of foreign priority date 12 January 2001.

2. Claims 1-2, 4-36, and 83-93 are currently pending in the application. Claims 1, 10, 21, 25, 29, and 33, are independent claims. Claims 51-82 are withdrawn. Claims 94-99 have been canceled, amendments to the claims are accepted.

Information Disclosure Statement

3. The IDS submitted 29 October 2007 has been considered.

Claim Objections

4. The Claim Objection is withdrawn due to amendment canceling claims 94-99.

Response to Arguments

5 Applicant's arguments submitted 10 October 2007 have been fully considered but they are moot due to new grounds of rejection below.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. **Claims 1-2, 4-7, 8, 20, 83-86,** are rejected under 35 U.S.C. 103(a) as being unpatentable over Scott et al. U.S. Patent No. 6,484,260 (hereinafter '260) in view of Bonneau et al. U.S. Patent No. 6,577,229 (hereinafter '229).

As to independent claim 1, "An authentication token which is normally held by a user and, when the user is to use a device for executing predetermined processing in accordance with authentication data of the user, connected to the device to perform user authentication on the basis of biometrical information of the user, comprising: a personal collation unit including a sensor for detecting the biometrical information of the user and outputting a detection result as sensing data, a storage unit which stores in advance registered data to be collated with the biometrical information of the user, and a collation unit for collating the registered data stored in said storage unit with the sensing data from said sensor and outputting a collation result as authentication data representing a user authentication result; a communication unit for transmitting the authentication data from said personal collation unit to the device as communication data, wherein said personal collation unit and communication unit are integrated" is taught in '260 col. 1, line 46 through col. 2, line 21;

the following is not explicitly taught in '260:

"and a protocol conversion unit for converting format of the communication data to be transmitted to the device into a format that can be received and decoded by the device that can be received and decoded by the device wherein said personal collation unit and communication unit are integrated" however '229 teaches that the device allows for additional smart card communication protocols to be added that service the smart card. In addition the functionality of the smart card communication device can be changed by a central computing system that is coupled to the smart card communication device in col. 4, lines 9-39.

I would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '260 a portable personal identification system utilizing biometrics to include a means to format the code sent as taught in '229. One in the art would have been motivated to perform such a modification because as indicated by '229 smart card technology is continually expanding in different directions (see '229 col. 2, lines 11 et seq.) "The smart card technology is continually expanding in different directions while various manufacturers and industries influence the implementation of smart card systems. As a result, numerous smart card communication protocols have been suggested and several protocols are currently in use. Regulatory and standard committees have defined several standard smart card protocols. For example, the International Organization for Standardization has provided at least two standards for proximity (also referred to as non-contact and contactless) smart cards: ISO 14443 Type A and ISO 14443 Type B. Although many conventional smart card systems use the same carrier frequency for communication, different communication protocols utilize different modulation techniques to transmit and receive data. For example, although ISO 14443 Type A and Type B both require a 13.56 MHZ carrier, ISO 14443 Type A systems use 100% ASK (Amplitude Shift Keying) modulation techniques and ISO 14443 Type B systems use 10% ASK modulation techniques to transmit data from the smart card communication device to the smart card. Further, the Type A smart card communication protocol requires ASK Manchester load modulation with a subcarrier at 847.5 kHz for transmission from the smart card to the smart card communication device. The Type B smart card communication protocol, however, dictates that the smart card transmit a signal modulated using Binary Phase Shift Keying--Non-Return to Zero (BPSK-NRZ) modulation with a subcarrier at 847.5 kHz".

As to dependent claim 2, "wherein said storage unit further stores in advance user information unique to the user, which is to be used for processing in the device, and said collation unit outputs the authentication data containing the user information read out from said storage unit" is shown in '260 col. 2, lines 15-43.

As to dependent claim 4, "further comprising a radio unit for transmitting the communication data from said communication unit to the device through a radio section" is taught in '260 col. 7, lines 35-58.

As to dependent claim 5, " further comprising a radio unit for transmitting the communication data from said protocol conversion unit to the device through a radio section" is shown in '260 col. 7, lines 35-38.

As to dependent claim 6, "further comprising a battery for supplying power" is disclosed in '260 col. 6, lines 29-39.

As to dependent claim 7, "wherein said battery comprises a secondary battery charged by power supply from the device when said authentication token is connected to the device" '260 teaches "Referring now to FIGS. 4A-4D, one embodiment of a PID 6B, which includes all the features also shown in FIG. 1, includes a housing 44 similar in size to a personal pager or a small cellular telephone" in col. 8, lines 14-40 it is obvious that a PID which is similar to a cellular phone would include rechargeable batteries.

As to dependent claim 8, "wherein said storage unit has, in addition to a storage area for storing the registered data, at least one storage area for storing another information" is taught in '260 col. 2, lines 27-38.

As to dependent claim 20, "wherein said authentication token further comprises another storage circuit for storing a password of said authentication token and token identification information for identifying said authentication token, and when the personal collation result indicates that the collation is successful, said communication unit transmits the password and token identification information in said another storage circuit to said service providing apparatus as the communication data" is taught in '260 col. 3, lines 49-63.

As to dependent claim 83, "wherein said token further comprises an encryption circuit for encrypting data generated from the authentication data and dynamic information generated by the device and transmitted using a key registered in advance, and said communication circuit transmits to the device encrypted data generated by said encryption circuit" is shown in '260 col. 2, lines 22-39;

"wherein the dynamic information changes each time it is generated" is disclosed in '260 col. 5, lines 49-58, because the random number changes with time.

As to dependent claim 84, "wherein said token further comprises a result determination circuit for, when the collation result indicates that the authentication is successful, outputting the authentication data to said encryption circuit, and when the collation result indicates that the authentication fails, outputting the authentication data to said first communication circuit, and an encryption circuit for, in accordance with the authentication data from said result determination circuit, encrypting dynamic

information transmitted from the device using a key registered in advance, adding obtained encrypted data to the authentication data, and outputting the encrypted data, and said communication circuit transmits to the device the authentication data with the encrypted data from said encryption circuit or the authentication data from said result determination circuit" is disclosed in '260 col. 2, lines 22-39.

As to dependent claim 85, **"wherein said token further comprises an encryption circuit for encrypting dynamic information transmitted from the device using a key registered in advance and outputting obtained encrypted data to said first communication circuit as data, and a first result determination circuit for, when the collation result indicates that the authentication is successful, instructing said encryption circuit to generate the encrypted data"** is taught in '260 col. 2, lines 53 through col. 3, line 3;

"and when the collation result indicates that the authentication fails, outputting data whose number of digits is different from that of the encrypted data that would be produced if the authentication was successful to said first communication circuit and said first communication circuit transmits to the device the data from said encryption circuit or the data from said first result determination circuit" is shown in '260 col. 3, lines 29-65 (note, Scott teaches if the authentication fails the process ends, this inherently means that the number of digits would be different).

As to dependent claim 86, **"wherein said token further comprises an ID storage circuit for storing identification information of said authentication token registered in advance, and said first communication circuit transmits to the device the identification information stored in said ID storage circuit"** is disclosed in '260 col. 3, lines 23-28.

8. **Claims 9-19, 21-36, and 87-93,** are rejected under 35 U.S.C. 103(a) as being unpatentable over Scott et al. U.S. Patent No. 6,484,260 (hereinafter '260) in view of Bonneau et al. U.S. Patent No. 6,577,229 (hereinafter '229) in further view of Sumino U.S. Patent No. 6,957,338 (hereinafter '338).

As to independent claim 10, "An authentication system for executing user authentication, which is necessary for use of a device for executing predetermined processing, by using biometrical information of a user, comprising: an authentication token which is normally held by the user and, when the user is to use said device, the authentication token connected to said device and to perform user authentication on the basis of the biometrical information of the user, said authentication token comprising a personal collation unit including a sensor for detecting the biometrical information of the user and outputting a detection result as sensing data, a storage unit which stores in advance registered data to be collated with the biometrical information of the user, and a collation unit for collating the registered data stored in said storage unit with the sensing data from said sensor and outputting a collation result representing a user authentication result as authentication data, a first communication unit for transmitting the authentication data from said personal collation unit to said device as communication data, and" is taught in '260 col. 1, line 46 through col. 2, line 21;

the following is not explicitly taught in '260:

"and a protocol conversion unit for converting format of the communication data to be transmitted to the device into a format that can be received and decoded by the device said personal collation unit and said first communication unit being integrated" however '229 teaches that the device allows for additional smart card communication protocols to be added that service the smart card. In addition the functionality of the smart card communication device can be changed by a central computing system that is coupled to the smart card communication device in col. 4, lines 9-39.

I would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '260 a portable personal identification system utilizing biometrics to include a means to format the code sent as taught in '229. One in the art would have been motivated to perform such a modification because as indicated by '229 smart card technology is continually expanding in different directions (see '229 col. 2, lines 11 et seq.) "The smart card technology is continually expanding in different directions while various manufacturers and industries influence the implementation of smart card systems. As a result, numerous smart card communication protocols have been suggested and several protocols are currently in use. Regulatory and standard committees have defined several standard smart card protocols. For example, the International Organization for Standardization has provided at least two standards for proximity (also referred to as non-contact and contactless) smart cards: ISO 14443 Type A and ISO 14443 Type B. Although many conventional smart card systems use the same carrier frequency for communication, different communication protocols utilize different modulation techniques to transmit and receive data. For example, although ISO 14443 Type A and Type B both require a 13.56 MHZ carrier, ISO 14443 Type A systems use 100% ASK (Amplitude Shift Keying) modulation techniques and ISO 14443 Type B systems use 10% ASK modulation techniques to transmit data from the smart card communication device to the smart card. Further, the Type A smart card communication protocol requires ASK Manchester load modulation with a subcarrier at 847.5 kHz for transmission from the smart card to the smart card communication device. The Type B smart card communication protocol, however, dictates that the smart card transmit a signal modulated using Binary Phase Shift Keying--Non-Return to Zero (BPSK-NRZ) modulation with a subcarrier at 847.5 kHz".

the following is not taught in the combination of '260 and '229: **"and said device comprising a second communication unit for receiving the communication data transmitted from said authentication token and outputting the data as the authentication data, and a processing unit for executing the predetermined processing on the basis of the collation result contained in the authentication data from said second communication unit"** however '338 teaches "a collating unit for respectively collating the biological information and the password output" in col. 1, lines 63-67.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '260 and '229 a portable personal identification system utilizing biometrics to include a means to store passwords in the personal devices as taught in '338. One in the art would have been motivated to perform such a modification because as indicated by '338 a need exist to combine the authentication cards used that store passwords with biometrics to insure security (see '338 col. 1, lines 32-51 "However, even in the individual authentication system using the IC card, if both the IC card (a physical object) and the password (individual knowledge) are stolen, the safety is not secured ... an object of the present invention is to provide an individual authentication system by which the data processing device which needs individual authentication can be used and managed with higher security".

As to dependent claim 12, **"wherein said storage unit of said authentication token stores in advance user information unique to the user, which is to be used for processing in said device, said collation unit of said authentication token outputs the authentication data containing the user information read out from said storage unit, and said processing unit of said device executes processing using the user information contained in the authentication data from said second communication unit"** is taught in '338 col. 1, lines 54-67. The motivation to combine '260 and '338 is the same as stated above in claim 10.

As to dependent claim 9, "wherein said at least one storage area for storing another information includes a storage area for storing personal information of the user and a storage area for storing service information" is shown in '338 col. 1, lines 54-67. The motivation to combine '260 and '338 is the same as stated above in claim 10.

As to dependent claims 11, 13-19, and 87-93,these claims contain substantially similar subject matter as claims 3- 9 and 83-86 above; therefore they are rejected along similar rationale.

As to independent claim 25, "An authentication method of executing user authentication, which is necessary when a user is to use a service providing apparatus for providing a predetermined service, between the service providing apparatus and provides the service to the user on the basis of a collation result and an authentication token for executing the user authentication using biometrical information of the user, wherein" is taught in '260 col. 1, line 46 through col. 2, line 21;

the following is not explicitly taught in '260:

"converts formats of communication data containing the password and token identification into a format that can be received and decoded by the service proving apparatus and

transmit the communication data to the service proving apparatus" however '229 teaches that the device allows for additional smart card communication protocols to be added that service the smart card. In addition the functionality of the smart card communication device can be changed by a central computing system that is coupled to the smart card communication device in col. 4, lines 9-39.

I would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '260 a portable personal identification system utilizing biometrics to include a means to format the code sent as taught in '229. One in the art would have been motivated to perform such a modification because as indicated by '229 smart card technology is continually expanding in different directions (see '229 col. 2, lines 11 et seq.) "The smart card technology is continually expanding in different directions while various manufacturers and industries influence the implementation of smart card systems. As a result, numerous smart card communication protocols have been suggested and several protocols are currently in use. Regulatory and standard committees have defined several standard smart card protocols. For example, the International Organization for Standardization has provided at least two standards for proximity (also referred to as non-contact and contactless) smart cards: ISO 14443 Type A and ISO 14443 Type B. Although many conventional smart card systems use the same carrier frequency for communication, different communication protocols utilize different modulation techniques to transmit and receive data. For example, although ISO 14443 Type A and Type B both require a 13.56 MHZ carrier, ISO 14443 Type A systems use 100% ASK (Amplitude Shift Keying) modulation techniques and ISO 14443 Type B systems use 10% ASK modulation techniques to transmit data from the smart card communication device to the smart card.

Further, the Type A smart card communication protocol requires ASK Manchester load modulation with a subcarrier at 847.5 kHz for transmission from the smart card to the smart card communication device. The Type B smart card communication protocol, however, dictates that the smart card transmit a signal modulated using Binary Phase Shift Keying--Non-Return to Zero (BPSK-NRZ) modulation with a subcarrier at 847.5 kHz".

the following is not taught in '260 and '229:

"the authentication token stores in advance a password of the authentication token and token identification information for identifying the authentication token, performs collation on the basis of the biometrical information detected from the user to check whether the user is an authentic user and when a collation result indicates that collation is successful" and **"and authentication token in advance in a first database in association with each other, collates the password contained in the communication data received from the authentication token with a password obtained from the first database using the token identification information as a key"** however '338 teaches "an individual authentication card for storing biological information and a password for identifying a registered user" (registered is interpreted to mean the information was provided in advance) in col. 1, lines 54-67.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '260 and '229 a portable personal identification system utilizing biometrics to include a means to store passwords in the personal devices as taught in '338. One in the art would have been motivated to perform such a modification because as indicated by '338 a need exist to combine the authentication cards used that store passwords with biometrics to insure security (see '338 col. 1, lines 32-51 "However, even in the individual authentication system using the IC card, if both the IC card (a physical object) and the password (individual knowledge) are stolen, the safety is not secured … an object of the present invention is to provide an individual authentication system by which the data processing device which needs individual authentication can be used and managed with higher security".

As to dependent claim 26, "wherein the token identification information and password are registered in the first database in association with each other from a registration apparatus connected to the service providing apparatus through a communication network" is disclosed in '260 col. 5, lines 55-58 "The personal identification device can be used in conjunction with conventional telephone lines or computer network communications".

As to dependent claim 27, "wherein the service providing apparatus causes a password generation circuit to generate a new password, transmits the new password to the authentication token through the second communication unit, and updates the password stored in the first database, and the authentication token updates the password stored in advance by the new password received from the service providing apparatus" is taught in '260 col. 3, lines 29-67 (note the generated random number is interpreted to have the same meaning as the new password).

As to dependent claim 28, "wherein the service providing apparatus stores device identification information for identifying the service providing apparatus in advance, and transmits the device identification information to the authentication token when the authentication token is connected, and the authentication token stores in advance the password and the device identification information for identifying the service providing

apparatus in a second database in association with each other, and uses, as the password to be transmitted to the service providing apparatus, a password obtained from the second database using the device identification information received from the service providing apparatus as a key" is shown in '260 col. 3, lines 29-67.

As to independent claim 29, this claim is directed to a recording medium for causing a computer to execute the authentication procedure of claim 25; therefore it is rejected along similar rationale.

As to dependent claims 30-32, these claims contain substantially similar subject matter as claims 26-28; therefore they are rejected along similar rationale.

As to independent claim 33, this claim is directed to a program for causing a computer to execute the authentication procedure of claim 25; therefore it is rejected along similar rationale.

As to dependent claims 34-36, these claims contain substantially similar subject matter as claims 26-28; therefore they are rejected along similar rationale.

As to independent claim 21, this claim contains the limitations previously presented in claims 1, 10, and 25; therefore it is rejected along similar rationale.

As to dependent claims 22-24, these claims contain substantially similar limitations as dependent claims 11, 27, and 28; therefore they are rejected along similar rationale.

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 7:30 am to 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen Tran

Ellen Tran
Patent Examiner
Technology Center 2134
20 December 2007